1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain **jointhemoment.net** using a Basic scan type. The analysis commenced on **April 18th at 03:00** and concluded in **00 hours, 12 minutes, and 33 seconds**. The scope of the work included a comprehensive evaluation of web application and infrastructure security, adhering to OWASP and OSCP methodologies. The primary focus was on identifying High and Medium-risk vulnerabilities that could impact the security posture of the domain.

1.2 Summary of Key Findings

The security assessment identified a total of **20 issues**, categorized as **2 High-risk**, **3 Medium-risk**, **2 Low-risk**, and **13 informational**. Critical findings include the presence of unencrypted HTTP traffic affecting **167 URLs**, posing significant risks of data interception and man-in-the-middle attacks, and SSL certificate expiration issues with one domain in critical status (**30 days remaining**) and another in warning status (**79 days remaining**). Medium-risk issues include the absence of Web Application Firewall (WAF) protection on **100%** of analyzed hosts, increasing vulnerability to cyber-attacks, and the detection of **4 login forms** requiring security validation. Immediate actions should focus on implementing HTTPS across all web applications, renewing SSL certificates promptly, and deploying WAF to mitigate potential threats.

1.3 Issues Table

Title	Risk
Unencrypted HTTP Traffic Detected	High
SSL Certificate Expiration Analysis	High
Absence of WAF	Medium
Nmap Port Scan Results Analysis	Medium
Login Form Detection Analysis	Medium
Shared Hosting Environment Analysis	Low
SSL/TLS Protocols Security Assessment	Low

1.4 Detailed Findings

1.4.1 Unencrypted HTTP Traffic Detected

Description:
A total of **167 URLs** were identified using unencrypted HTTP protocol, which exposes data to interception and man-in-the-middle attacks. This lack of encryption compromises data integrity and authenticity, failing to meet security compliance requirements.

Affected Assets:
- All identified URLs using unencrypted HTTP protocol.

Recommendations:
Implement HTTPS across all web applications to ensure data is encrypted during transmission. Utilize HSTS (HTTP Strict Transport Security) to enforce secure connections and prevent protocol downgrade attacks.

1.4.2 SSL Certificate Expiration Analysis

Description:
SSL/TLS certificates for two domains are nearing expiration. The certificate for **www.jointhemoment.net** is in a critical state with only **30 days remaining**, while **jointhemoment.net** has **79 days remaining**, classified as a warning.

Affected Assets:
- jointhemoment.net - www.jointhemoment.net

Recommendations:
Renew the SSL/TLS certificates immediately to maintain secure communications. Implement automated monitoring for certificate expiration to prevent future lapses.

1.4.3 Absence of WAF

Description:
Both hosts analyzed lack Web Application Firewall (WAF) protection, resulting in a **100% vulnerability rate**. This absence increases the risk of successful cyber-attacks, particularly injection-based attacks.

Affected Assets:
- jointhemoment.net - www.jointhemoment.net

Recommendations:
Deploy a Web Application Firewall to protect against common web application attacks such as SQL injection and cross-site scripting (XSS). Regularly update WAF rules to adapt to emerging threats.

1.4.4 Nmap Port Scan Results Analysis

Description:
The scan detected **4 open ports**, including port 80 running HTTP without encryption. This poses a risk if not redirected to HTTPS or if HSTS is not enabled.

Affected Assets:
- IP Address: **34.249.241.152**

Recommendations:
Ensure all HTTP services are redirected to HTTPS. Enable HSTS to enforce secure connections and prevent protocol downgrade attacks.

1.4.5 Login Form Detection Analysis

Description:
A total of **4 login forms** were detected across the application, indicating potential security risks if not properly secured.

Affected Assets:
- Various URLs associated with detected login forms.

Recommendations:
Implement strong authentication mechanisms such as multi-factor authentication (MFA). Ensure login forms are protected by HTTPS to prevent credential interception.

1.5 General Recommendations

To enhance the overall security posture, it is recommended to implement a comprehensive security strategy that includes regular vulnerability assessments, timely patch management, and continuous monitoring of security controls. Additionally, fostering a culture of security awareness among employees can significantly reduce the risk of human error leading to security breaches.